Cyber Disorders:

Rivalry & Conflict in a Global Information Age

Lucas Kello

Science, Technology & Public Policy Program
International Security Program
Minerva Project (Harvard-MIT)

Belfer Center, Harvard Kennedy School

Purpose

- Discuss effects of cyber weapons on patterns of rivalry and conflict in international system
- Premised on following assumptions:
  a) Related technologies pose significant risks to security and in some respects have destabilizing, possibly transforming effects on patterns of relations
  b) These risks and effects widely recognized and constantly referred to by security planners
  c) Yet little systematic analysis which subjects cyber weapons and new modes of behavior they enable to empirical and theoretical evaluation from an international relations perspective

Contents

Significance to Policymakers

- Security planners widely recognize significance of cyber threat to national and international security:
  - "America's **economic prosperity** in the 21st century will depend on cybersecurity...And this is also a matter of **public safety** and **national security**. We count on computer networks to deliver our oil and gas, our power and our water...[The] cyber threat is **one of the most serious economic and national security challenges** we face as a nation."

    (Barack Obama, May 2009)
  - "Cyber threats will soon pose the **greatest threat** to our country."

    (Robert Mueller, Mar 2012)
  - "Prior to 9/11, there were all kinds of information out there that a **catastrophic attack** was looming. The information on a cyberattack is at that same frequency and intensity and is bubbling at the same level, and we should not wait for an attack in order to do something."

    (Janet Napolitano, Mar 2012)
  - "[Cyberwar] is **just as critical to military operations** as land, air, and sea."

    (William Lynn III, 2012)

Significance to Policymakers

- "Cyber attack, including by other states, and by organized crime and terrorists…[are] of the **highest priority** for national security looking ahead, taking account of both the likelihood and impact." A **"Tier 1"** threat
  - **equal** in priority to a CBRN attack by terrorists
  - **above** a CBRN or conventional attack by another state

  (UK Security Strategy, 2010)
- "A large-scale [cyber]attack on NATO's…energy grids could possibly lead to **collective defense** measures under **Article 5**."

  (Albright Report, May 2010)

- Global security expert opinion:
  - 36% believe cybersecurity more important than missile defense
  - 45% believe cybersecurity as important as border security
  - 57% believe a "cyber arms race" is taking place

  (McAfee/SDA, 2012)

Response of IR Community

- General reaction has been to shrink before the cyber peril owing to its technical intricacies or novelties or both
- Survey of literature (Reardon & Choucri 2012) illustrates the **scholarship gap**
  - 18 IR journals in period 2001-10 examined
  - 49 articles on cyber politics in just 6 publications
  - Neglect especially pronounced in peer-reviewed academic journals (only 16 articles)
  - Focus of nascent empirical theory on topics not directly related to security implications of cyber weapons
  - Governance of cyberspace and role of public/private, national/international institutions (ITU, ICANN, IETF, etc.)
  - Political economy of Internet and digital technologies as drivers of growth
  - Information revolution and germination of a global civil society

State of Analysis

- Only 5 articles centering on cyber conflict and security:
  - Goldman 2004, Eriksson & Giacomello 2006, Hansen & Nissenbaum 2009, Manjikian 2010, Newmyer 2010
- Security related topics include
  - Disruptive or destructive cyberattacks
  - Cyberespionage and theft of military technology/secrets
  - Social media and authoritarian regime stability (eg, Arab Uprisings)
- All the while, policymakers anticipate a threat evolution towards greater disruptive and destructive use of cyber weapons

- Strategic studies of cyber weapons are at a conceptually similar stage as nuclear studies in 1950s – while pace of events closer to 1960s (Nye 2011)

Policymaker's Dilemma

- Implication: Cybersecurity policy based on theoretical axioms that have outlived their validity
- This is no surprise
  - Threats to security are **immediate** – so too must policy response be swift
  - Practitioners have little time to absorb novel technologies into theoretical suppositions
  - This is an essentially scholarly task involving a slow **learning process**
  - Requires **body of experience** on which to draw suppositions – yet this remains small
  - Nonetheless, basic features and patterns of rivalrous cyber conduct can be detected (Part 3)

Bases of Neglect

- Attitude of resignation among IR community amounts to one or both of two assertions
  1. that the problem is not of sufficient scale to warrant close inspection
  2. that only technical experts are equipped to assess magnitude of problem or provide suitable remedies

  - In brief, the cyber peril is either **not significant** or **not comprehensible** to political scientists

Argument of Insignificance

- Three central claims (Rid 2012, Rid & McBurney 2012):
  a) Cyberattacks not potentially violent and do not meet definition of "act of war" – consequently, are unimportant to international security
  b) Destructive attacks are unlikely because of high costs and technical difficulties
  c) Collateral damage not significant

- Scope and nature of threat exaggerated:
  – Stuxnet was "the world's first **cyber super weapon**..." (CSM, Nov 2010)
  – "a **digital missile** and a **cyber-Hiroshima bomb**." (CSM, Jan 2012)
  – "The US faces potential of cyberattack equivalent to **Pearl Harbor**."

(Leon Panetta, Aug 2011)

Argument of Insignificance

- Incentives to exaggerate magnitude of the threat
  - "There's a **power struggle** going on in the US government right now. It's about who is in charge of cyber security, and how much control the government will exert over civilian networks. And by beating the **drums of war**, the military is coming out on top." (Bruce Schneier, Jul 2010)
- Presumed seriousness of cyber threat based on
  - Unsubstantiated anecdotal evidence
  - Knowledge of our own (US) capabilities inferred upon adversaries
- Thus, "cyberwar" is not "already upon us" (as claimed by Clarke 2010, Arquilla 2012)

Argument of Inscrutability

- Stresses following obstacles to research:
  - Little reliable incident data – major **methodological** impediment
    - Overclassification of cyberattacks by government
    - Underreporting by private sector
  - No clear or agreed metrics for assessing **vulnerabilities** to or **damage** from cyberattack (vulnerabilities usually not known until actually manipulated, ie, “zero-day”)

Costs of Resignation

- Result is absence of **structured debate** – both empirical and theoretical – on implications of cyber weapons for national and international security
- Given prominence of cyber threat in policy discourse, scholars have **obligation** to integrate new technologies into theories and concepts of IR
  - Skeptics must articulate theoretical and empirical grounds of dissent as basis for alternate policy course
  - Believers must leverage theoretical tools to support and improve prevailing policy
- Costs of resignation are double:
  - Diminished security in practice
  - Stagnation and decreased relevance of theory
- IR community effectively ceding cybersecurity analysis to technologists and practitioners
- Result is "hypertechnologism" and explosion of cyber politics in absence of theories and concepts to give it coherence

Contents

Technical Fundamentals

- Conceptual toolkit of cybersecurity analysis limited and problematic
  - At technical level, misunderstanding of basic properties of information technologies
  - Conceptually, confusion and discord in use of key terms which have different implications for security policy

- **Aims:**
  - Provide basic technical and conceptual understanding of cyberspace and threats propagating through it in order to address argument of inscrutability
  - Propose selection of common concepts to guide structured debate and design of empirical theory

- **Premise:** Much of attitude of resignation in IR derives from absence of such a basic framework

7 Key Concepts

1. **Cyberspace:** "A global domain within the information environment consisting of the network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DoD)

- Three subcomponents (some overlapping):
  - Internet (TCP/IP)
  - World Wide Web
  - Critical information infrastructures (incl. systems **not** connected to Internet)
- Implications for security policy:
  - Not all threats propagating through WWW can transmit through Internet
  - Not all threats transmissible via Internet can use it to reach "air-gapped" CIIs
- Two kinds of cyberattack targets:
  - "Remote access"
  - "Closed access"

7 Key Concepts

- Conceptual muddlement:
  - NSPD-54 (Jan 2008) conflates cyberspace and Internet
    - Describes "cyberspace" as "the interdependent network of information technology infrastructures"
    - Yet closed-access systems not interdependent at logical or information layers
  - Germany's *Cybersecurity Strategy* (2011) contradicts itself
    - "Cyberspace is the virtual space of all IT systems linked at data level on a global scale…IT systems in an isolated virtual space are **not** part of cyberspace."
    - Yet: "Experience with the Stuxnet virus shows that important [and isolated] industrial infrastructures are no longer exempted from targeted IT attacks."

7 Key Concepts

2. **Cybersecurity:** Measures taken to protect a computer system or network – and the social, economic, governmental functions supported by them – against unauthorized access or disruption
   - Security **within** cyberspace
   - Security **from** cyberspace
- Can also be viewed as a state of affairs
- Alternate interpretation (China, Russia): "Information security"
- Fundamental tension between **security** and **utility** of a computer system:
  - Only means to secure system absolutely is by severing all vectors of access (and thus attack) to it
  - This renders system futile in transmission of data – very purpose of information technologies
  - Dilemma: A system that is impregnable is useless to those wanting to utilize it legitimately; if accessible, it is manipulable by adversaries seeking to inflict harm
  - Thus, neither absolute safety nor absolute convenience attainable

7 Key Concepts

3. **Malware:** Software designed to interfere with normal operations of a computer system or network
   - A **tool** of cyberattack – not an instance or class of it
   - Example of conceptual confusion: "Malware" as distinct category of "cyber incidents" (Cavelty 2012)

4. **Cybercrime:** Crime involving use of a computer system or network
   - Typically involves data theft (eg, credit cards) or transmission (child porn)
   - Because criminal law is unenforceable against states, focus is on non-state agents prosecutable in domestic jurisdictions (eg, CoE "Cybercrime Convention")
   - Not a principal concern of national or international security

5. **Hacktivism:** Use of cyber instruments for political or ideological purposes
   - Usually by private actors (sometimes with Letter of Marque)
   - Can be exploitation (data theft) or attack (disruption)

7 Key Concepts

6. **Cyberexploitation:** Penetration of an adversary's computer system or network to seize information (NRC 2009)
   - Essentially an intelligence-gathering activity
   - Eg: Ghostnet, Operation Aurora
   - No reason to impute disruptive or destructive intent

7. **Cyberattack:** Deliberate disruption of a computer system or network and functions delivered or supported by it (NRC 2009)

- Two important distinctions:
  a) **Cyber as adjunct** to conventional force (Syria 2007) v. **cyber-only** attack (Stuxnet)
  b) **Generalized** (Estonia 2007) v. **customized** attack (Stuxnet)

7 Key Concepts

- Successful exploit or attack both require three things (NRC 2009):
  a) **Vulnerability** to manipulate
  b) **Access** to vulnerability
  c) **Payload** to deliver intended effect
- Nature of payload differentiates the two

Multiple Confusions

- Practitioners & media often conflate exploitation and attack or ignore distinction:
  - "[T]he semantics of defining cybercrime [usually exploit] v. cyberwar [high-caliber attack] are largely irrelevant." (Alex Seger, CoE, Feb 2012)
  - "Cyberwar [with Wikileaks] will hit all users." (BBC, Dec 2010)
  - "[T]here are two principal policy areas in cybersecurity that have particular relevance for cyberwarfare: First, there are measures intended to combat cyberattacks (including cybercrime/cyberterrorism)..." (European Parliament report, 2011)
  - "Cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber espionage." (Germany's *Cybersecurity Strategy*, 2011)

A Conceptual Starting Point

- Technically, exploits and attack can be similar – ie, utilize same access vector and manipulate same vulnerability
- Operationally, successful attack often relies on exploitation (Stuxnet)
- Yet implications of each for policy and law very different:
  - Cyberexploitation by governments breaches domestic but not international law
  - Cyberattacks have at least in principle potential to be "armed attack" under UN Article 51 or NATO Article 5
- Exploit-attack distinction crucial to security studies; consequently, the two should not be conflated
- Propose to adopt conceptual distinction into basic terminology of cyber IR scholarship

Contents

Cyber Rivalry & Conflict

- **Aims:**
  - Address argument of insignificance in three steps:
    1) Assess growing vulnerabilities to cyberattack
    2) Discuss tangibility of cyberattack effects
    3) Review proliferation of cyber weapons in international system
  - Provide preliminary reflections on implications of cyber rivalry for IR

1. Vulnerabilities

- Network surface of defender vast and expanding
  - Use of software to support societal functions pervasive – growing exposure to cyberattack
  - Hardware vulnerabilities and supply-chain risks
  - Increase in systems complexity raises costs of customized attack – but costs of defense also rise
  - Stuxnet shows that costs of high-caliber attack high – but costs of defense higher
- Architecture of Internet and design of services delivered or supported by it consistently prioritize ease of use over security (Brenner 2011)
- Evident in design principles of "ARPANET" (Clark 1988)
  - Fundamental goal: Survivability of communications
  - Secondary goals: Accountability and security
  - Priority was packet delivery, not authentication of contents or sender's identity

1. Vulnerabilities (Cont.)

- Government systems vulnerable to attack
  - 90% of US government traffic runs through private ISPs
  - Penetration of government systems up by 650% since 2006 (DHS)
- CII connectivity (power grids, air-traffic control, financial networks, etc.)
  - Run electronically via SCADAs – digitally manipulable
  - Utilize public telecomms backbone – remote access vectors via Internet
  - Increasingly rely on global supply chain – off-shelf and off-shore software/hardware risks
  - Many critical systems *already* penetrated
    - Problem of adversary permanently residing in our networks
    - Possibility of dormant attack payloads in case of war or crisis
    - 1917 Battle of Messines as historical analogy

1. Vulnerabilities (Cont.)

- **Root paradox of cybersecurity:** Societies most adept at harnessing cyberspace for social and economic gain are those most exposed to dangers propagating through it – "flight into cyberspace" expresses vulnerability as much as strength
- Poll of Western experts:
  - 61% anticipate impact of extended loss of connectivity would be "catastrophic"
  - 69% doubt their countries' ability to defend against sophisticated attack

(EastWest Institute, Jan 2011)

2. Tangibility

- Dispel presumption of weapons' virtuality:
  - Only access vector and vulnerability manipulation "virtual"
  - Payload effects may be tangible – even kinetic
  - US "equivalence doctrine" an expression of this – permits conventional retaliation to cyberattack
- Two basic kinds of cyberattack effects:
  - **"Direct":** Within unitary logical environment, incl. functions supported by system (SCADA disruption, centrifuge destruction, etc.)
  - **"Indirect":** Beyond logical environment (cascading economic loss, psychological damage, etc.)
- Offensive cyber power can be used for strategic and political ends outside cyberspace
  - Support to conventional military force (Georgia 2008)
  - Substitute to conventional force (Stuxnet)
  - Nonmilitary political and strategic ends (Estonia 2007)
  - Ideological and religious extremism (al Qaeda?)

2. Tangibility (Stuxnet)

- Customized to affect industrial control system at uranium enrichment plant in Natanz, Iran
- Access vector: Removable USB drives to bridge “air gap”
- Vulnerabilities: Four “zero-days” and two stolen digital certificates
- Mode of operation:
  - Uploaded own malicious code, transmitting from user machines to SCADA via internal network
  - Hid injected code from controller, preventing operator from detecting unauthorized commands
  - Payload understood and manipulated logic of controller
    - Altered rotational speed of IR-1 centrifuges, causing physical impairment
    - Marked decrease in centrifuge trends at Natanz (IAEA)
- Tactical significance of Stuxnet disputed
- Strategically, however, slowed uranium enrichment in context of broader diplomatic initiative to halt suspected nuclear weapons program – may have prevented unilateral Israeli airstrike (Sanger 2012)

3. Proliferation

- Barriers to entry into cyber arena low (Nye 2010)
- Disruptive cyber weaponry cheap compared to conventional tools and is attractive for perceived power-equalizing effects
- States and nonstate actors can play significant role in cyber conflict
  - Over 100 state actors presently developing virtual stockpiles
  - Number of hacktivist actors like Anonymous able and willing to inflict harm likely inestimable

- Together, growing vulnerabilities, tangibility of attack payloads, and weapons' proliferation mean that **consequences** and **likelihood** of cyber conflict both likely to rise

Cyber Weapons: Transforming or Not?

- Many practitioners perceive Information Age as “new” or “revolutionary” era
- But what does break mean for IR and strategic thinking?
- Certain observations can be drawn – even if implications limited largely to cyber domain and validity provisional until further data available

5 Implications for IR

1. Cyber weapons empowering actors with nontraditional motives and aims
   - "Power diffusion" is increasing ability of **nonstate** actors to inflict harm (Nye 2010)
   - Multiplication of adversaries willing and able to act in absence of (or against) government direction requires us to problematize state-centric logics of behavior
   - However, assumption of **state-centrism** holds in key respects:
     - Governments principal players in cyber domain, esp. for Stuxnet-like cyberattack
       - Deep intelligence capability for payload customization
       - Human resources to discover vulnerabilities and open attack vector
     - "Security" still conceived in national terms (against Der Derian 2003)

5 Implications for IR

2. Decreasing territoriality of Westphalian state
   - Many forms of malicious behavior not prosecutable in national courts
   - Digital dependence eroding key boundaries:
     - Between national/economic security
     - Between public/private actors (eg, China employs thousands of civilian hackers)
   - Nevertheless, much of physical backbone of Internet resides within state jurisdictions and is susceptible to government influence

5 Implications for IR

3. Cyber rivalry is straining "anarchical society" among states
   - Most IR scholars tacitly presuppose existence of element of "society":
     - Common interests in **elementary goals**
     - **Rules** prescribing conduct which sustains goals
     - **Institutions** helping to make rules effective
   - New actors empowered by cyber tools not sharing in elementary goals and values of international society
     - Eg: "Love Bug" 2000 forced closure of email at CIA, Pentagon, UK Parliament – perpetrated by lone hacker in Philippines
   - Multiplication of relevant players complicates arrival at consensus on rules and norms to regulate permissible uses of cyber weapons
     - Will nonstate actors comply with interstate rules?
     - If not, how to impose compliance?
   - Capacity of existing legal and normative frameworks to absorb new technologies and actors empowered by them does not seem promising

5 Implications for IR

4. Disruption of stable patterns of international interaction
   - Absence of agreed or clear rules and norms can have destabilizing effects on **strategic interactions**
   - Imprecise **"cause-effect" knowledge**: Cyber weapons so new and vulnerabilities they seek to manipulate so complex as to impede interpretation of probable effects in their use
     - Eg: Iraq 2003, Stuxnet, Libya 2011
   - Problem of **"blowback"**: When a negative effect returns to hit instigator
     - Directly, through self-propagative tendencies of malware
     - Indirectly, through cascading economic damage
   - No known or tested **escalatory logics** for cyber exchange
     - No Confidence Building Measures
     - Unclear signaling procedures
     - No agreed standards of "proportionality" in response to attack
     - Problem of unsanctioned intervention by nonstate actors
     - Little concurrence of values or interests to reinforce expectancy of behavior in crisis

5 Implications for IR

5. Imprecise knowledge of assailant
   - Much of IR logics premised on assumption that adversary's identity can be plausibly ascertained
   - But different to kinetic weapons, cyber weapons can be used with high degree of anonymity
   - Technically difficult to authenticate identity and location of cyberattacker (NRC 2009):
     - **Accuracy:** Is attribution correct?
     - **Precision:** Russia → FSB → 16th Directorate?

- Summary of attribution problem:
  - If you cannot identify perpetrator, cannot impose penalties
  - If we think we know, may not be sure to actionable degree of certitude
  - By time we are certain, may be too late to avert or reverse strategic setback
  - Weakens deterrence, which requires certain attribution (to evade penalties of misattribution or legitimacy costs in retaliation)

Doctrinal Quandaries

- Cyber weapons present problems for inherited security doctrines
- Four basic postulates challenged:
  a) that offensive power is identifiable and measurable (cyber arms verification is difficult)
  b) that it is readily discernible from defensive power (how to ascertain nature of payload before weapon actually used?)
  c) that its possession only by states or largest among these truly matters (power diffusion)
  d) that its employment can be reasonably attributed, predicted, modelled (attribution problem and imperfect cause-effect knowledge)

Closing Remarks: Cyber Disorders

- Emergent realities of cyber rivalry placing foundations of political order in anarchy under strain
- In international cyber domain
  a) not all relevant actors fully known or recognized
  b) little concurrence of elementary goals, interests, and rules among them
  c) increasingly disorderly interaction
- Broad picture that emerges:
  - Dynamics of cyber rivalry interacting with traditional interstate relations, which persists in various forms
  - Cyber domain will continue to host familiar games of states, even while enabling nontraditional actors to intervene in and possibly disrupt interstate dealings

Closing Remarks: Cyber Disorders (Cont.)

- There are in effect two **"states of nature"** to grapple with:
  - Traditional one between states confronting recognized adversaries and locked in familiar modes of competition but with new instruments at their disposal (eg, Stuxnet)
  - That of incipient "global" system characterized by growing multiplicity of nonstate actors with variant motives, capabilities, opportunities to inflict harm (eg, Estonia 2007)
- Greatest potential for **chaos** may be in instances where two "states of nature" collide – where high stakes of interstate competition encounter irregularities and disturbances of nonstate activity

- Conditions that will restore orthodoxies of anarchic international politics may not be within immediate reach
- Return to normality and stability will require political action and instruments
- For this, a **political science** of cyber IR is essential

Foundational theory → Empirical theory → Theory of praxis

Works Cited

Arquilla, J. 2012. “Cyberwar Is Already Upon Us.” *Foreign Policy* (March/April)

Brenner, J. 2011. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime & Warfare*. London: Penguin

Cavelty, M.D. 2012. “The Militarization of Cyber Security as a Source of Global Tension.” *Strategic Trends 2012: Key Developments in Global Affairs*. Zurich: ETH

Clark, D. 1988. “The Design Philosophy of the DARPA Internet Protocol.” *Computer Communication Review* 18(4): 106-14

Clarke, R. 2010. *Cyber War: The Next Threat to National Security & What to Do About It*. New York: HarperCollins

Der Derian, J. 2003. “The Question of Information Technology in International Relations.” *Millennium* 32(3): 441-56

Eriksson,J. & Giacomello, G. 2006. “The Information Revolution, Security, and International Relations: (IR)relevant Theory?” *International Political Science Review* 27(3): *221-44*

Goldman, E.O. 2004. “Introduction: Information Resources and Military Performance.” *Journal of Strategic Studies* 27(2): 195-219

Works Cited (Cont.)

Hansen, L. & Nissenbaum, H. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly 53(4):* 1155-75

Manjikian, M.M. 2010. "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik." *International Studies Quarterly* 54(2): 381-401

National Research Council. 2009. *Technology, Policy Law & Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC

Newmyer, J. 2010. "The Revolution in Military Affairs with Chinese Characteristics." *Journal of Strategic Studies* 33(4): 483-504

Nye, J.S. 2010. "Cyber Power." Paper, Belfer Center for Science & International Affairs, Harvard Kennedy School

_____. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter): 18-38

Reardon, R. & Choucri, N. 2012. "The Role of Cyberspace in International Relations: A View of the Literature." Paper presented at the ISA Annual Convention

Works Cited (Cont.)

Rid, T. 2012. “Think Again: Cyberwar.” *Foreign Policy* (March/April)

Rid, T. & McBurney, P. 2012. “Cyber-Weapons.” *The RUSI Journal* 157(1): 6-13

Sanger, D. 2012. *Confront & Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers